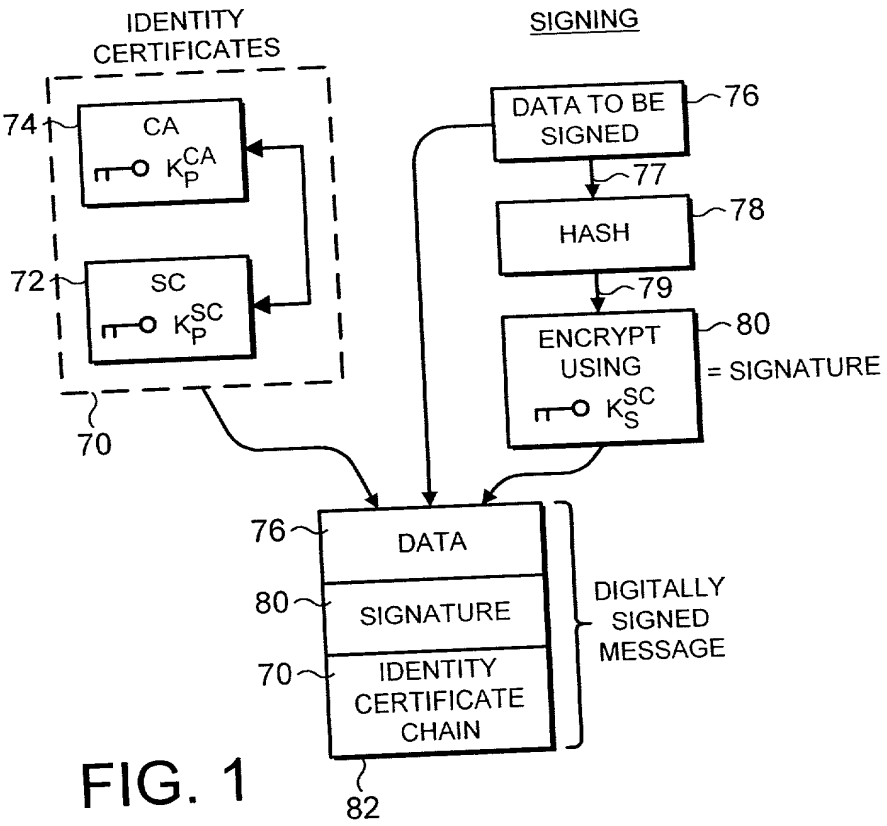
IDENTITY CERTIFICATES
SIGNING
74
CA
K_P^{CA}
72
SC
K_P^{SC}
70
DATA TO BE SIGNED
76
77
HASH
78
79
ENCRYPT USING
K_S^{SC}
80
= SIGNATURE
76
DATA
80
SIGNATURE
70
IDENTITY CERTIFICATE CHAIN
DIGITALLY SIGNED MESSAGE
82

FIG. 1

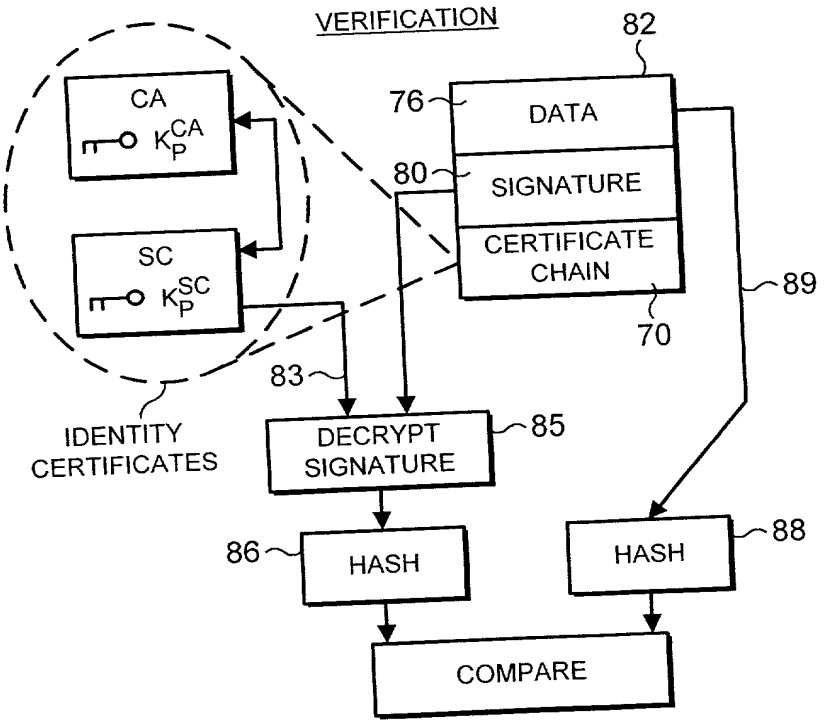
VERIFICATION
82
CA
K_P^{CA}
SC
K_P^{SC}
76
DATA
80
SIGNATURE
CERTIFICATE CHAIN
70
89
83
IDENTITY CERTIFICATES
DECRYPT SIGNATURE
85
86
HASH
HASH
88
COMPARE
IF EQUAL → OK
ELSE BAD SIGNATURE

FIG. 2

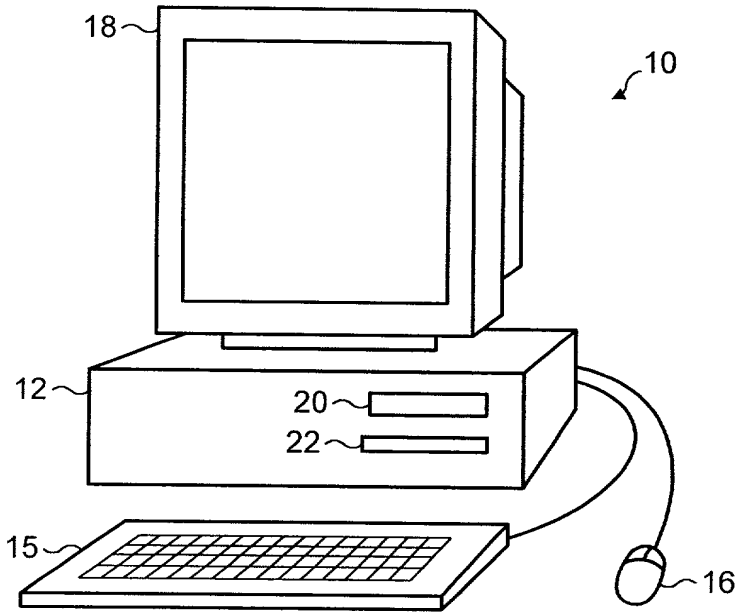

FIG. 3

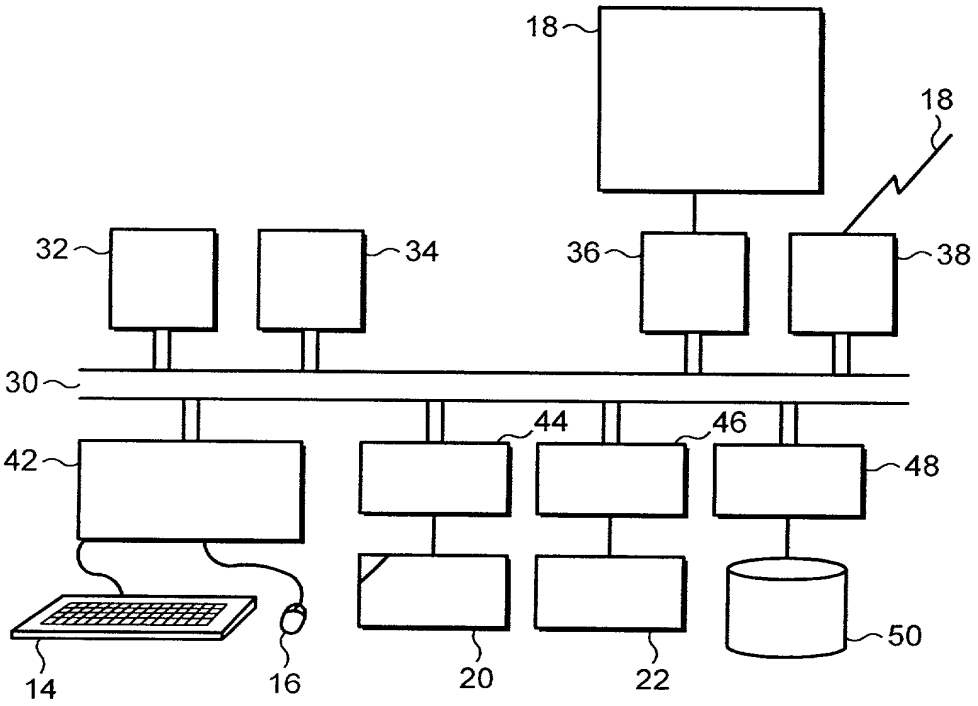

FIG. 4

Attorney Docket No. 95-4926

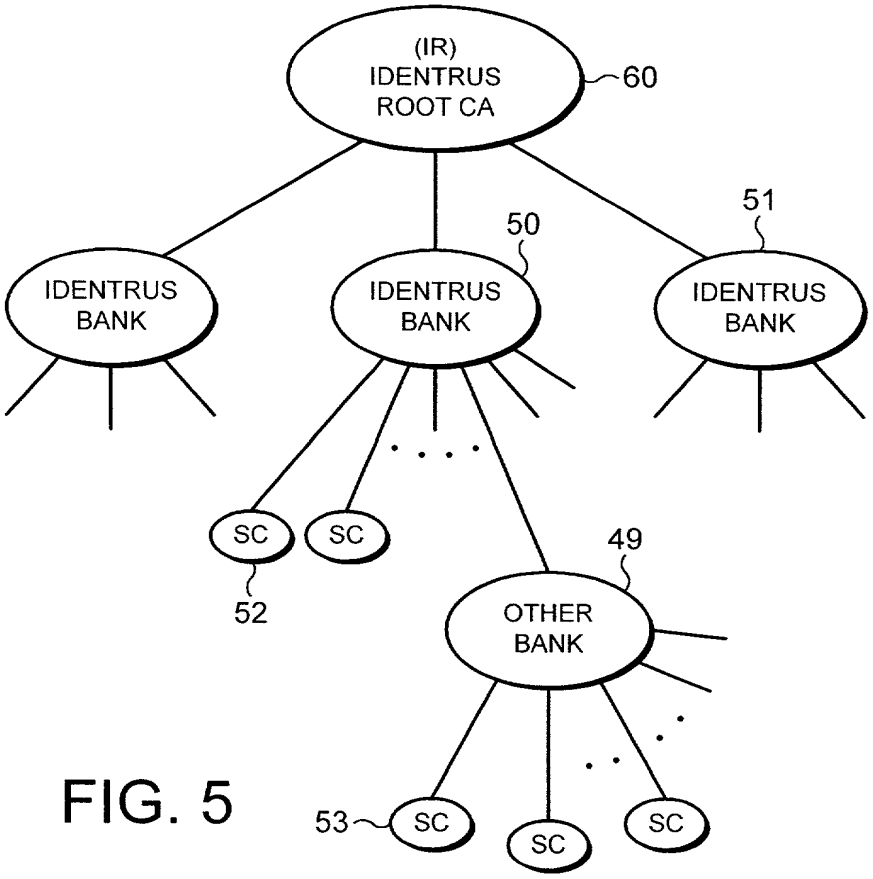
(IR)
IDENTRUS
ROOT CA
60
IDENTRUS
BANK
IDENTRUS
BANK
IDENTRUS
BANK
50
51
SC
SC
52
49
OTHER
BANK
53
SC
SC
SC

FIG. 5

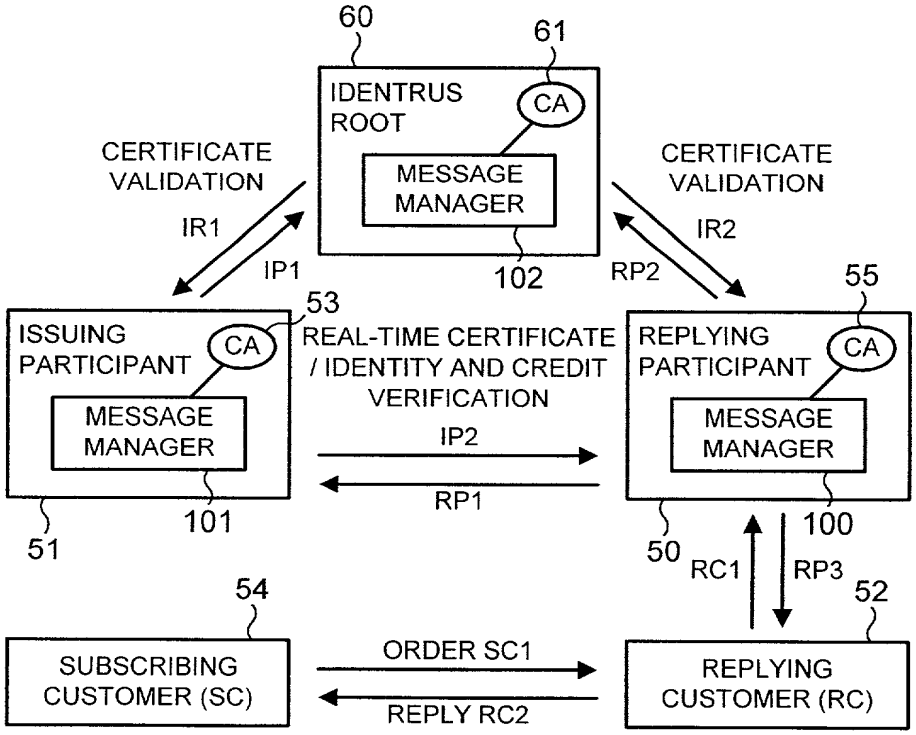
60
61
IDENTRUS
ROOT
CA
MESSAGE
MANAGER
102
CERTIFICATE
VALIDATION
IR1
IP1
CERTIFICATE
VALIDATION
IR2
RP2
55
53
ISSUING
PARTICIPANT
CA
MESSAGE
MANAGER
101
51
REAL-TIME CERTIFICATE
/ IDENTITY AND CREDIT
VERIFICATION
IP2
RP1
REPLYING
PARTICIPANT
CA
MESSAGE
MANAGER
50
100
RC1
RP3
52
54
SUBSCRIBING
CUSTOMER (SC)
ORDER SC1
REPLY RC2
REPLYING
CUSTOMER (RC)

FIG. 6

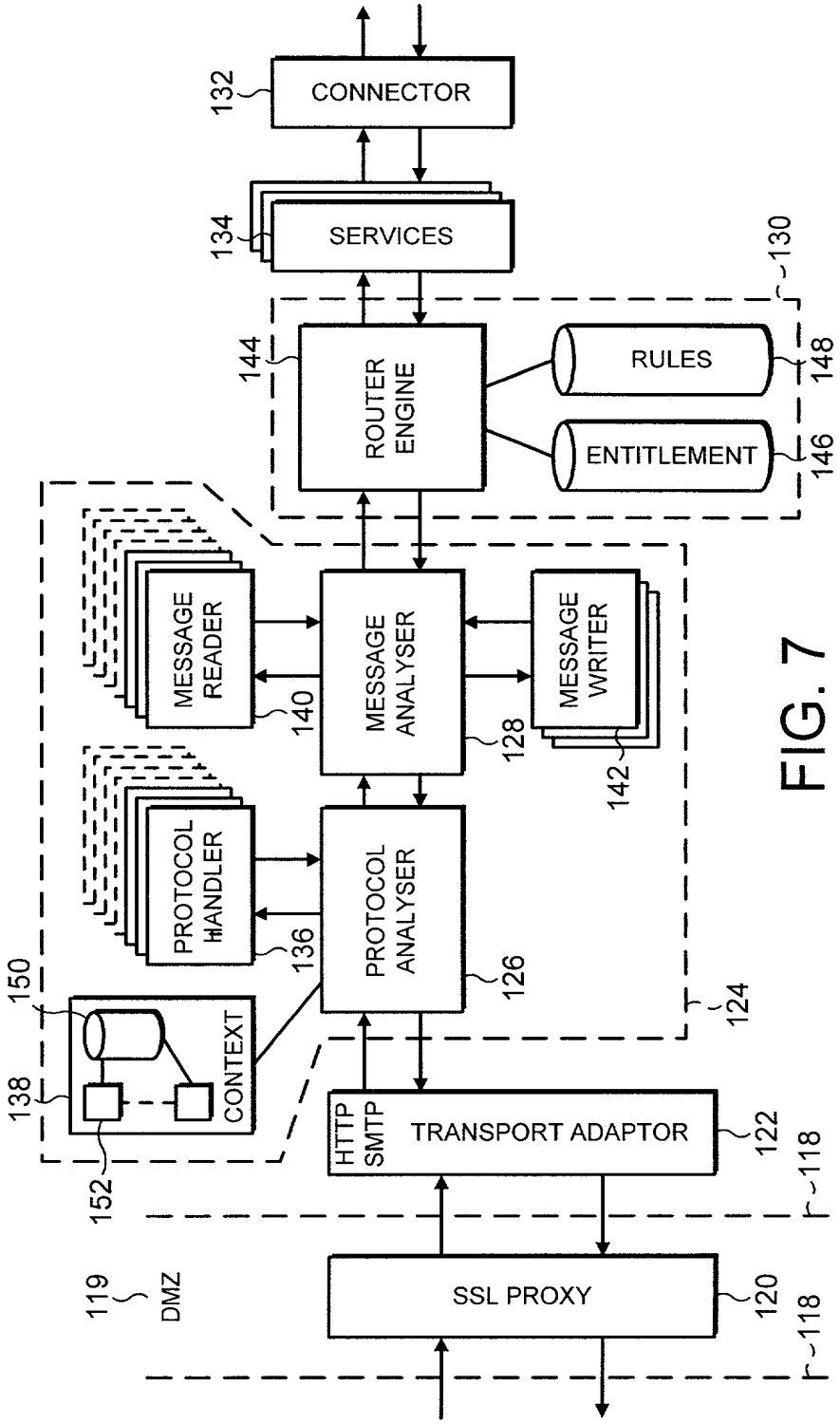
CONNECTOR
132
SERVICES
134
130
ROUTER ENGINE
144
RULES
148
ENTITLEMENT
146
MESSAGE READER
140
MESSAGE ANALYSER
128
MESSAGE WRITER
142
PROTOCOL HANDLER
136
PROTOCOL ANALYSER
126
124
150
CONTEXT
138
152
HTTP SMTP
TRANSPORT ADAPTOR
122
118
119
DMZ
SSL PROXY
120
118

FIG. 7

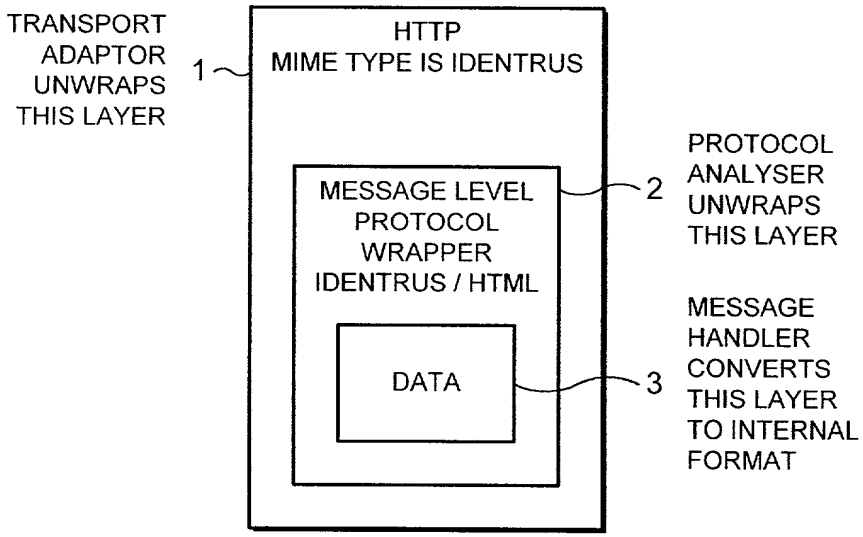
TRANSPORT
ADAPTOR
UNWRAPS
THIS LAYER
1
HTTP
MIME TYPE IS IDENTRUS
MESSAGE LEVEL
PROTOCOL
WRAPPER
IDENTRUS / HTML
DATA
2
3
PROTOCOL
ANALYSER
UNWRAPS
THIS LAYER
MESSAGE
HANDLER
CONVERTS
THIS LAYER
TO INTERNAL
FORMAT

FIG. 8

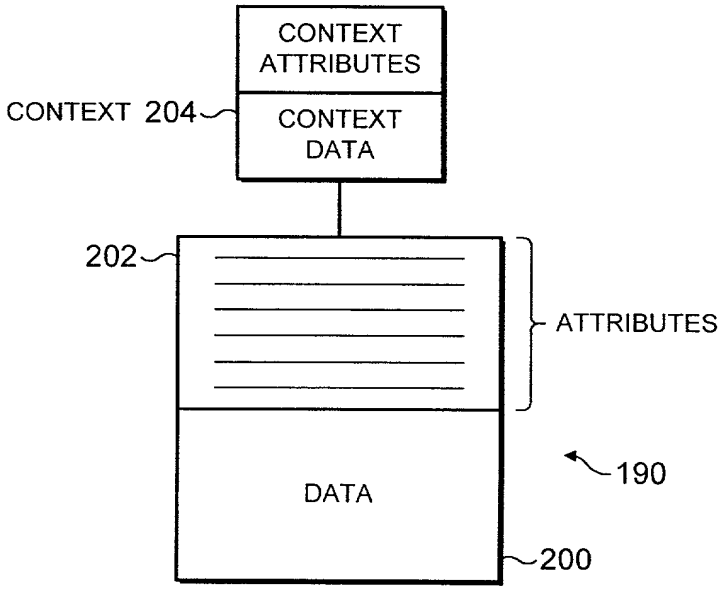
CONTEXT
ATTRIBUTES
CONTEXT 204
CONTEXT
DATA
202
ATTRIBUTES
DATA
190
200

FIG. 9

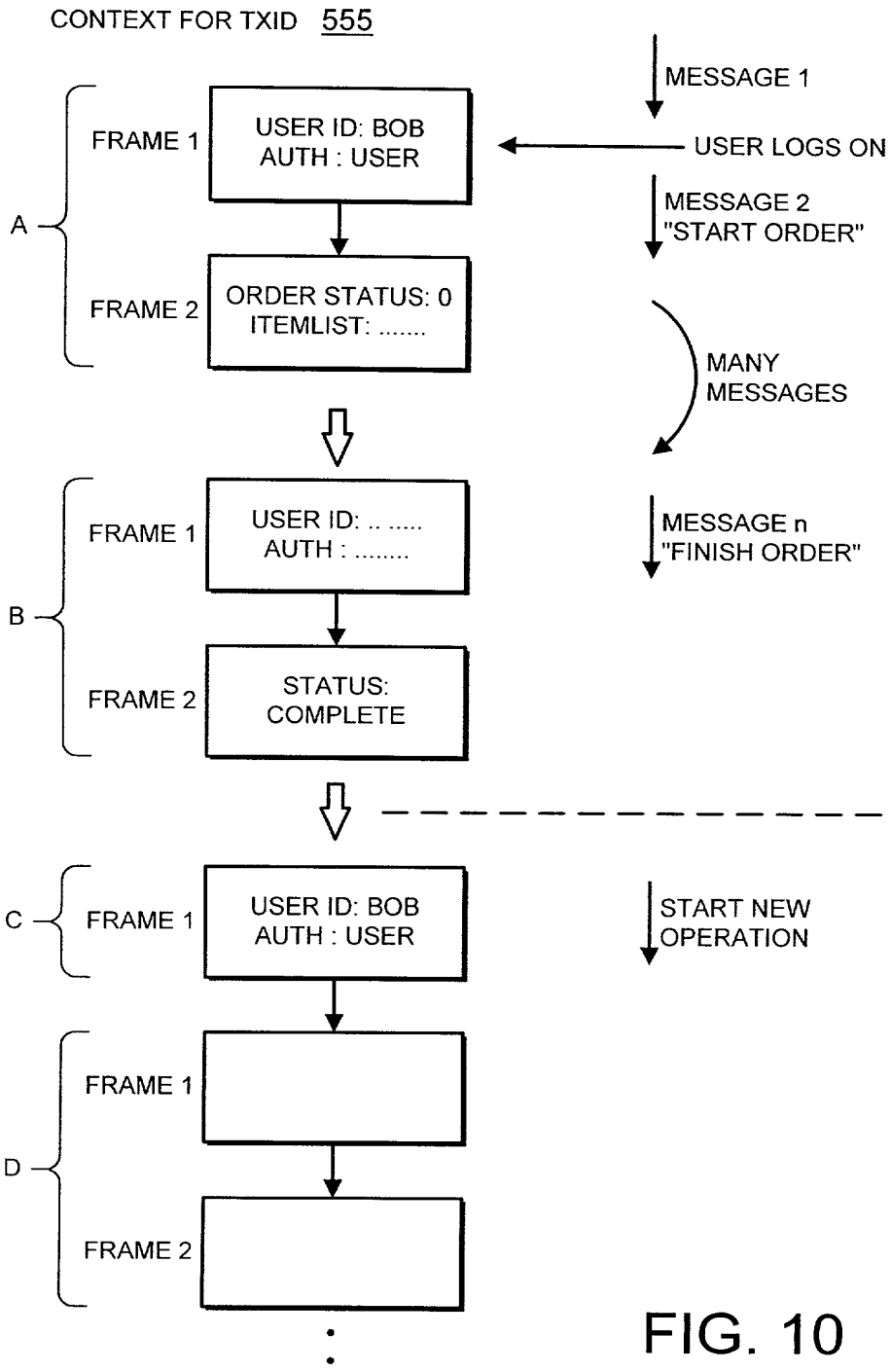
CONTEXT FOR TXID 555
MESSAGE 1
USER LOGS ON
MESSAGE 2
"START ORDER"
MANY
MESSAGES
MESSAGE n
"FINISH ORDER"
START NEW
OPERATION
A
FRAME 1
USER ID: BOB
AUTH : USER
FRAME 2
ORDER STATUS: 0
ITEMLIST: .....
B
FRAME 1
USER ID: .. ..
AUTH : .....
FRAME 2
STATUS:
COMPLETE
C
FRAME 1
USER ID: BOB
AUTH : USER
D
FRAME 1
FRAME 2

FIG. 10

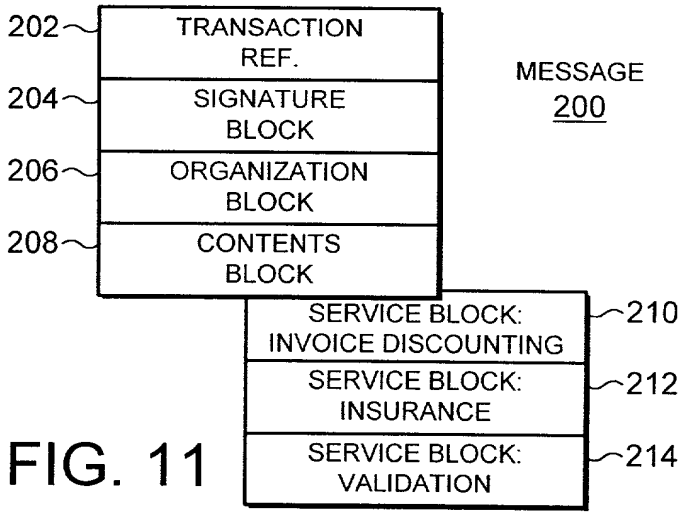
202
TRANSACTION REF.
204
SIGNATURE BLOCK
206
ORGANIZATION BLOCK
208
CONTENTS BLOCK
MESSAGE
200
SERVICE BLOCK: INVOICE DISCOUNTING
210
SERVICE BLOCK: INSURANCE
212
SERVICE BLOCK: VALIDATION
214

FIG. 11

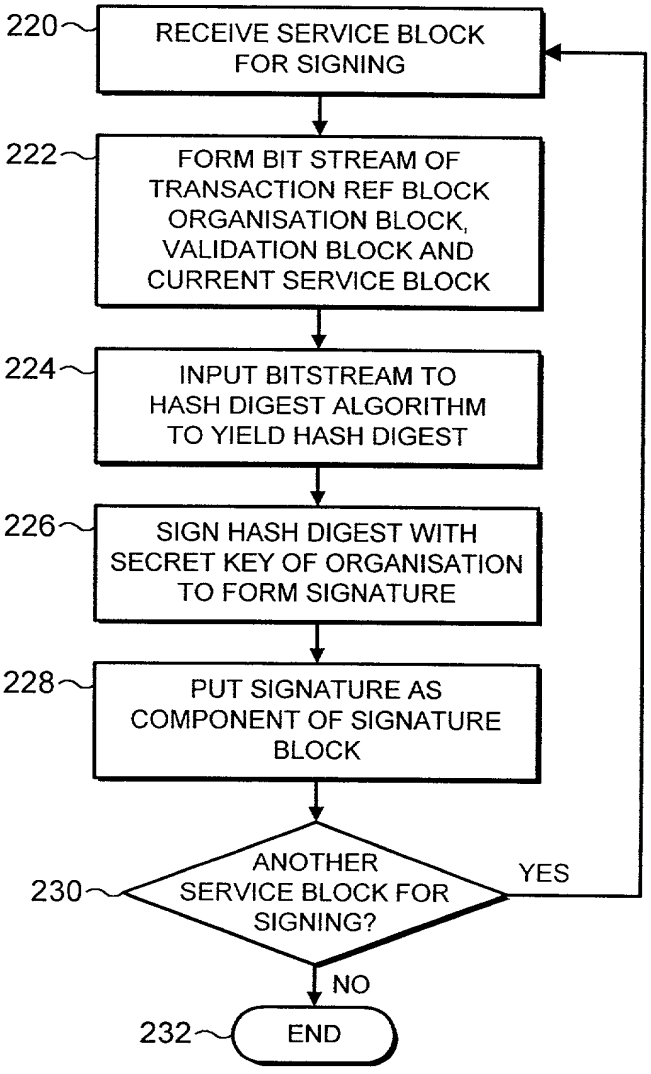
220
RECEIVE SERVICE BLOCK FOR SIGNING
222
FORM BIT STREAM OF TRANSACTION REF BLOCK ORGANISATION BLOCK, VALIDATION BLOCK AND CURRENT SERVICE BLOCK
224
INPUT BITSTREAM TO HASH DIGEST ALGORITHM TO YIELD HASH DIGEST
226
SIGN HASH DIGEST WITH SECRET KEY OF ORGANISATION TO FORM SIGNATURE
228
PUT SIGNATURE AS COMPONENT OF SIGNATURE BLOCK
230
ANOTHER SERVICE BLOCK FOR SIGNING?
YES
NO
232
END

FIG. 12

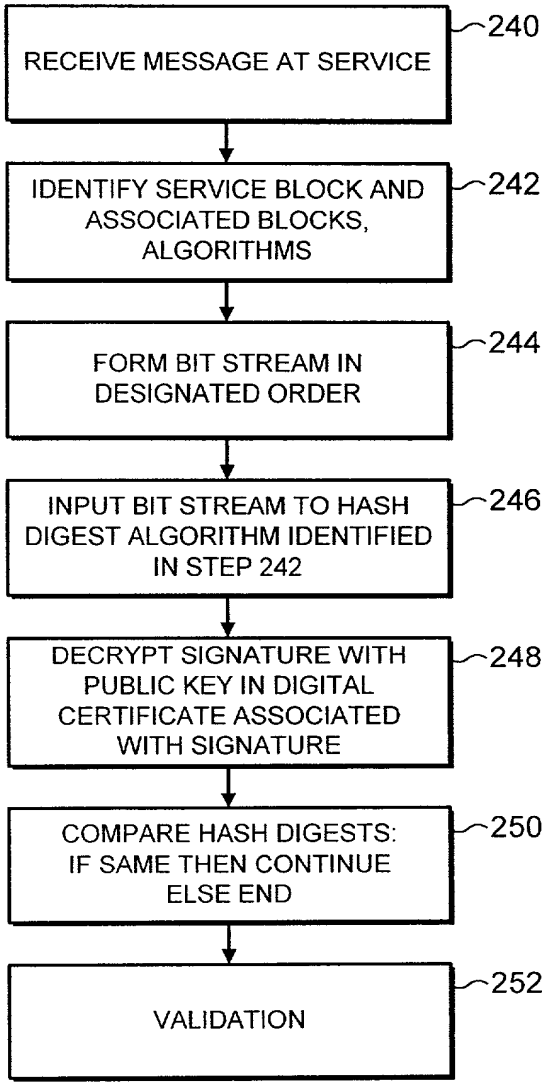
RECEIVE MESSAGE AT SERVICE
240
IDENTIFY SERVICE BLOCK AND ASSOCIATED BLOCKS, ALGORITHMS
242
FORM BIT STREAM IN DESIGNATED ORDER
244
INPUT BIT STREAM TO HASH DIGEST ALGORITHM IDENTIFIED IN STEP 242
246
DECRYPT SIGNATURE WITH PUBLIC KEY IN DIGITAL CERTIFICATE ASSOCIATED WITH SIGNATURE
248
COMPARE HASH DIGESTS: IF SAME THEN CONTINUE ELSE END
250
VALIDATION
252

FIG. 13

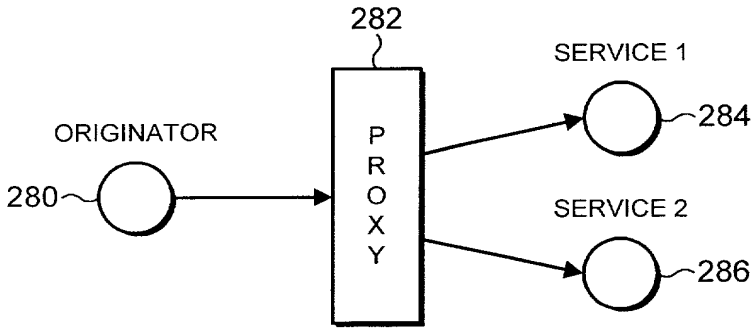
282
SERVICE 1
284
ORIGINATOR
280
PROXY
SERVICE 2
286

FIG. 14